Protection against threats during system design

S.P.I.R.I.T
- ✓ **Independence**
- ✓ **Perseverance**

Monday, 04 April 2022

Learning Intention

To develop knowledge by
Describing methods of identifying vulnerabilities

To secure understanding by
Explaining different ways of protecting software systems during design, creation, testing and use

To achieve excellence by
Condensing information into a suitable form

Hacking
unauthorized access to data in a system or computer.

Tier 2 word – vulnerability
is the quality of being easily hurt or attacked

Measures to Protect System

Make notes on the following

- Penetration testing
- Network forensics
- Role of Cookies

Requires a definition for each. All keywords underlined or highlighted

Learning Intention

To develop knowledge by
Describing methods of identifying vulnerabilities

To secure understanding by
Explaining different ways of protecting software systems during design, creation, testing and use

To achieve excellence by
Condensing information into a suitable form

Penetration Testing

- Penetration testing is a sub set of ***ethical hacking*** that deals with the process **of testing a computer system, or network to find vulnerabilities that an attacker could exploit**.

- The tests can be automated with software applications or they can be performed manually.

https://www.youtube.com/watch?v=q2t91jLmh3k

To develop knowledge by
Describing methods of identifying vulnerabilities

To secure understanding by
Explaining different ways of protecting software systems during design, creation, testing and use

Penetration Test Strategies

Targeted testing, testing carried out by the organization's IT team and the penetration testing team working together.

External testing, to find out if an outside attacker can get in and how far they can get in once they have gained access.

Internal testing, to estimate how much damage a dissatisfied employee could cause.

Blind testing, to simulate the actions and procedures of a real attacker by severely limiting the information given to the team performing the test.

Examples – that could be tested

Buffer overflow attacks - where data inside an overflow buffer (temporary data storage area) intentionally contains codes designed to change data, or disclose confidential information.

- Thorough testing, particularly of any library routines used, will help to prevent this type of attack.

Permissions Every time you want to install an app you are asked to give permission for the software to access certain settings and features of your device (e.g. give them access to personal data etc).

- App developers need to consider the scope of access and limit the number of permissions required at the design stage.

Scripting restrictions Same Origin Policy (SOP) is a security measure that prevents a web site's scripts from accessing and interacting with scripts used on other sites which could potentially contain malicious scripts, leading to malware infections or sensitive data being compromised.

Accepting parameter without validation Dynamically generated HTML pages can introduce security risks if inputs are not validated on the way in.

- Malicious script can be embedded within input that is submitted to web pages.
  validation rule are designed that will check and filter input parameters.

Network Forensics

Definition

Monitoring and analysis of network traffic to detect intrusion.

Analysts will search for data that points towards human communication, manipulation of files, and the use of certain keywords for example.

There are **two** methods of overarching network forensics

- "**catch it as you can**" method, which involves **capturing all network traffic** for analysis, which can be a long process and requires a lot of storage.
- "**stop, look and listen**" method, which involves **analysing each data packet** flowing across the network and only **capture** what is deemed as **suspicious** and worthy of extra analysis; this approach can require a lot of processing power but does not need as much storage space.

Cookies

- Cookies are data stored on a computer system.
- They allow websites to store a small amount of uniquely identifying data on your computer system while you are visiting.

    e.g a website can then identify you in future without requesting that you identify yourself each time, i.e. by entering a username and password

https://www.youtube.com/watch?v=rdVPflECed8

Cookies can be seen as a security issue as they **hold personal information** and this can be used or sold and tracking cookies can hold information on the websites visited by users.